(12) INTERNATIONAL LICATION PUBLISHED UNDER THE PATENT ERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 May 2004 (13.05.2004)

PCT

(10) International Publication Number
WO 2004/040397 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/SE2003/001660

(22) International Filing Date: 27 October 2003 (27.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/422498 31 October 2002 (31.10.2002) US

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL.) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: SMEETS, Bernard [NL/SE]; Dalbackavägen 11, S-240 10 Dalby (SE). SELANDER, Göran [SE/SE]; Bergsundsgatan 25, S-117 37 Stockholm (SE). NERBRANT, Per-Olof [SE/SE]; Katarinavägen 2D, S-184 51 Österkär (SE).

(74) Agent: AROS PATENT AB; P.O. Box 1544, S-751 45 Uppsala (SE).

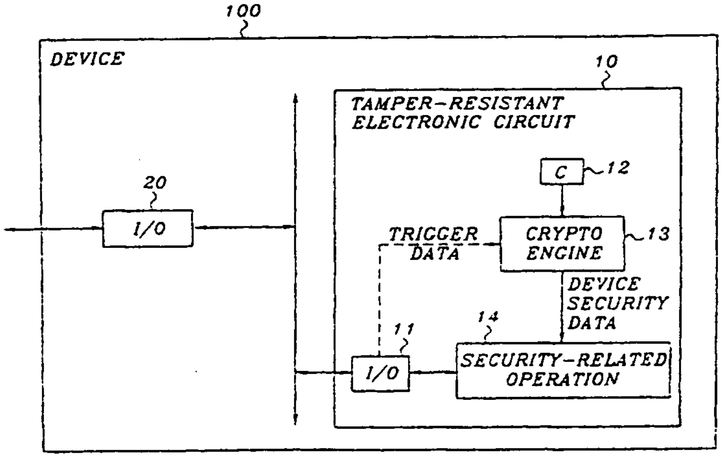
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, EG, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE IMPLEMENTATION AND UTILIZATION OF DEVICE-SPECIFIC SECURITY DATA



(57) Abstract: The invention concerns a tamper-resistant electronic circuit (10) configured for implementation in a device (100). The electronic circuit (10) securely implements and utilizes device-specific security data during operation in the device (100), and is basically provided with a tamper-resistantly stored secret (C) not accessible over an external circuit interface. The electronic circuit (10) is also provided with functionality (13) for performing cryptographic processing at least partly in response to the stored secret to generate an instance of device-specific security data that is internally confined within said electronic circuit (10) during usage of the device (100). The electronic circuit (10) is further configured for performing one or more security-related operations or algorithms (14) in response to the internally confined device-specific security data. In this way, secure implementation and utilization device-specific security data for security purposes can be effectively accomplished. The security is uncompromised since the stored secret (C) is never available outside the electronic circuit, and the device-specific security data is internally confined within the circuit during usage or operation of the device.